Legitimate by design

Whitworth, B.; de Moor, A.

Published in:
Proceedings of the 35th HICSS

Publication date:
2002

LEGITIMATE BY DESIGN: TOWARDS TRUSTED VIRTUAL COMMUNITY ENVIRONMENTS[1]

Brian Whitworth[2]
New Jersey Institute of Technology
bwhitworth@acm.org

Aldo de Moor
Tilburg University, The Netherlands
ademoor@kub.nl

Abstract. ***Legitimacy is a key part of the social requirements specification for a trusted virtual community environment (VCE). If an environment is not seen as legitimate, social conflicts may reduce community benefits like trade and e-commerce. Legitimacy must be built into a VCE at design time, or it may not be possible at all. This can be done using a legitimacy requirements framework (LRF) which interprets historical "rights" in terms of ownership of generic VCE objects. This involves more than merely specifying who has the right to do what to what, because objects may contain other objects, objects may be dependent, rights may interact, groups may have rights, and there may be rights to rights. A LRF could be used by software designers to derive legitimacy requirements for a wide variety of multi-user systems, from chat rooms to virtual realities. It would draw focus to common problems, and aid their common solution. A simple LRF is presented to provide a basis for designers of virtual social environments to copy, discuss or deviate from.***

Introduction

Traditional information system (IS) are *tools* individuals use to solve external problems like calculating a budget. Modern multi-user applications, including the Internet, are social *environments*. The person is represented within the software, as well as acting upon it. The "user" seems less the individual than the group or community. The software is a *virtual community environment* (VCE) that must satisfy the needs of the community. Satisfying virtual community technical requirements, like bandwidth, has revealed equally necessary underlying social requirements. Today the main problem such software faces is the *social-technical gap* - the difference between social needs/expectations and computer system capability [1]. Internet privacy concerns are a conflict between social requirements and current Internet system design. The community social requirement is for *legitimacy* – that internal dealings between people are fair and reasonable. Other examples are copyright, censorship, trespass, intellectual property, libel and even "rape" in virtual spaces. Increasingly, the problem today's IS designers face is what *can* be done than what *should* be done, what is legitimate rather than what is feasible. Social requirements, like legitimacy, will change the nature of software design over the next decade.

Virtual community. A virtual community (VC) is a self-sustaining group, with persisting social practices, acting in a common computer-mediated space. Groups are self-sustaining when the benefits of internal interaction, such as gaining knowledge, making friends, or belonging to a group, make members *want* to remain. It is not just a task group that stops when the task is complete, or a "rent-a-crowd" that requires payment. Temporary collections of people are also not communities. It is not merely the people that persist, but their form of interaction, their social environment, which can continue even if people come and go. A community is also *a form of self-sustaining group interaction that endures*. The formation of large, stable communities is a feature of human social evolution [8].

Virtual community environment. The computer-mediated "space", within which people act (and interact) is the virtual community environment (VCE). A VCE is an information system (IS), not a virtual community, nor does a VCE's existence guarantee a virtual community will arise. A bulletin board will be the basis of a virtual community only if lasting and common social practices develop. More general terms are groupware and cyberspace. *Groupware* is any software that allows computer-mediated interaction, whether communities or not. *Cyberspace* is computer-mediated interaction of any sort, not necessarily between people.

---

[1] This paper was published in the Proc. of the 35th Hawaii International Conference on System Sciences, Hawaii, January 7-10, 2002.

[2] This work was supported in part by the New Jersey Information-Technology Opportunities for the Workforce, Education and Research (NJ I-TOWER) Project, funded by the New Jersey Commission on Higher Education (contract #01-801020-02)

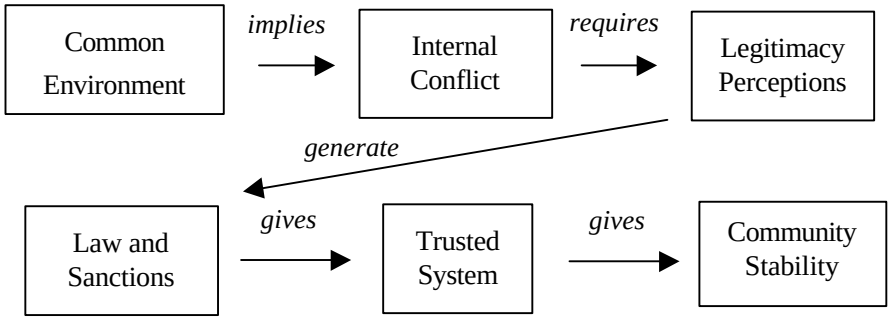

Figure 1. Legitimacy as means of resolving internal community conflict

Social value. To be self-sustaining, a community must generate social value for its members [24]. This value is the benefits of group interaction less the costs. The cognitive three process (C3P) model proposes that group members interact with factual information, each other, and the group, using distinct processes (of analyzing, relating and belonging) [38]. The direct individual benefits of community then are gaining knowledge, relating to others, and belonging to a group. On a group level the three processes generate informational, personal and normative influence. The latter allows communities to be governed by implicit and explicit social norms, which prescribe the affordances and constraints of acceptable communal behavior [31]. However legitimacy seems less about creating social benefits than minimizing the cost of social conflict.

Social conflict. In a common environment, the actions of one person may affect another. Whenever two or more people wish contrary actions involving the same environment object(s) there is the potential for inter-personal conflict. For example in a physical community, members share the same roads, and for one driver to proceed at an intersection, perhaps another must wait. If both parties proceed (seeking an individual advantage) they will come into conflict (i.e. "crash"), as the environment cannot satisfy both their demands. Such conflict often damages (and costs) not only the acting parties, but others as well. For the group, the effect is usually a net loss, so a group weakened by internal conflict tends not to last. A stable community requires some way to resolve internal conflict without member confrontations.

Legitimacy. Developed human societies try to avoid internal "lose-lose" conflicts using a complex set of "rights" - common expectations of who can do what and when. If conflicts are resolved by right not might the group is strengthened. Legitimacy is a *social perception, common to a group, used to resolve situations of internal group conflict*, usually expressed in terms of what is "right" or "fair", or what is "wrong" or "unfair". Legitimate actions are acceptable to the community [7]. It can be considered a group evolutionary social adaptation to a problem (conflict), rather than a moral or ethical issue. A stable society requires a fair system of social interaction, and the case has been well made that justice is an implementation of the concept of fairness [25]. A legitimate environment follows fair procedures, called in psychology procedural justice [19], and studies show people will avoid unfair situations [2], and often prefer fairness even when it does not maximize their personal benefit [19]. The development and implementation of legitimate social environments seems a necessary condition for groups to persist and form communities.

Law. Law is the formal statement of legitimacy concepts as group rules to resolve social conflict. Hence law cases always involve two parties in conflict (prosecution and defense). Legitimacy is the social perception that precedes the law, and is the sense used to form laws. It allows judges and juries to make precedent decisions, where the law is unclear.

Legality. Legality, whether an action is according to law, is not equivalent to legitimacy. An action seen as illegitimate may not be illegal if no law exists (e.g. virtual rape). And a legitimate action could be illegal (e.g. a bad law). What is "right" varies over time and between cultures. Legitimacy is situated, not a specific social practice. A dictatorial community is as legitimate as a democratic one if the group accepts their dictator as rightfully so.

Sanctions. Sanctions are actions taken by, or on behalf of, communities to enforce their laws (e.g. by police). A common sanction is group rejection by banishment or imprisonment. Though legitimacy is the common perceptions

that precede law, sanctions (and police) must still enforce it, as knowing what is right is not doing it. Individuals may *act* illegitimately, through need or greed, but still *know* their actions are wrong. Those who knowingly commit illegal acts are criminals. What is at stake is their community membership and liberty. When people feel the law is illegitimate (e.g. suffragettes for women's rights) they are revolutionaries. What is at stake now is the community itself, which may be destabilized if the core conflict is not resolved.

Trusted systems. A trusted social system is one in which legitimate rights are implemented [32]. Locke first made explicit that people have a natural right to the fruits of their labor [20]. If some people take the trouble to grow flowers, most agree it is not right that passers by pick them for their benefit. This is not considered "fair". This concept can be implemented in various ways - by laws and police, by a fence, by norms, or any combination. If the implementation is successful (and flowers are not stolen) the environment becomes a trusted one, and gardeners will find it worthwhile to grow flowers. However if people routinely pick other people's flowers, gardeners will tend not to bother to grow them (because others will only steal them). In this case, neither the gardeners nor the thieves have flowers, i.e. the group as a whole loses. The same logic can be applied to any constructive endeavors. Hence the driving force behind legitimacy is that it benefits the whole community [6]. Trusted online communities are critical to generating the benefits of community interaction, like trade, and "e-business" is simply trade in a virtual environment [30, 37]. Progress in legitimacy, (e.g. slavery, human rights, women's rights) leads to economic growth and prosperity, as people in trusted systems contribute, purchase, provide, and generally participate more. When systems are seen as legitimate, people self-regulate, and do not have to be forced (by police) to do things [35]. Simply put, *legitimacy benefits the entire community*.

Security. Trusted systems have two aspects: legitimacy and security. If security ensures that a system is used as intended, legitimacy defines that intent. For example, whether a user is who they say they are (authentication), is a security issue. What rights they *should* have is a legitimacy issue. Considerable effort has gone into ensuring online interactions are secure. This is good, but in generating trust and business, no amount of security can compensate for a lack of legitimacy, as police states illustrate.

Summary. Figure 1 summarizes these concepts. Multiple actors in a common environment means potential social conflict. Legitimacy perceptions allow commonly accepted laws and sanctions, that usually resolve internal conflicts. This gives a trusted system which is stable and prosperous. Legitimacy is thus a foundation stone of any enduring community.

Research question

If legitimacy is as critical to virtual as physical communities, the question that arises is *how to design legitimate virtual community environments*. In traditional single user software legitimacy is not a problem, but multi-user software changes all that.

Current situation. Today's Internet users often behave more like hunter-gatherers than societies. In any environment, people naturally move to valued resources, e.g. a gold-rush. For a community to evolve more is required, or when the resource is gone, the people leave. In the new world of cyber-space, the main resource is information. But people gathered around an information "gold-mine" is not a community. Information gold-diggers are notoriously fickle, and many online environments developed with the assumption that communities would automatically form [28], have found that after an initial honeymoon, members drift away, and most struggle to last beyond a year [29]. Often virtual community web sites are obituaries. A single unpleasant conflict can destroy an otherwise thriving community [17 p81]. A study of AOL new subscribers found that nearly all joined to communicate with members of pre-existing communities, and only 10% of continuing users used AOL to generate new friends [13]. Virtual society seems still in its infancy, perhaps a similar to the "Wild West" in the US 100 years ago, with an equal need for community development.

Legitimacy issues recur. When communities form, conflicts of interest and group rules tend to follow. The original Internet designers suggested a community without rules, a Utopian free society, with no laws, where everyone did as they wished. They created a system where authorship was not recognized, and while traditional painters can sign their work in a unique manner, cyber-artists cannot. Who would have thought when the Internet was being designed that ownership would become the issue it is today? The Napster dispute is an example. Copyright was supposed to die, but the Commerce Department's 1995 White Paper suggests we are entering an era when copyright may be

more protected than ever before [17]. Rather than social practices following technologies lead, copyright is being reinstated in the online environment [32]. If the original Internet architecture had included signature and public/private data fields, authors could have designated their creations as public or private, and browsers could respect that choice [16]. Acrobat 5.0 now uses a digital signature to return to document owners their copy rights. Legitimacy problems are inherent in social situations, and when ignored do not go away, but simply resurface at a later date.

Legitimacy issues are widespread. Today's concern is that software companies will reinstate their own rights (of property) but ignore their customer's rights (of privacy). The Orwellian monitoring and control systems possible in the "brave new worlds" of virtuality could be a "great leap backwards" socially, and privacy groups have sprung up in response. Stephen Manes puts the conflict well: "*Private lives? Not ours! 'You have zero privacy anyway.' Sun Microsystems' CEO Scot McNealy said last year. 'Get over it.' He's right on the facts, wrong on the attitude*." [22]. "The attitude" is the view of some corporates that "Your information belongs to us.". Rather than getting over it, people are more likely to do, eventually, what they always do: demand legitimate rights. An example is the Intel's inclusion of a Processor Serial Number (PSN) in its Pentium III in 1999. Users felt strongly that it was not right for application software to access a unique identity number on their computer without their consent. Privacy, the right to personal information, is a legitimacy issue, and legitimacy prevailed when Intel disabled the feature. The argument that author ownership benefits the group has also been well made for privacy, i.e. that *privacy is a public good* [26]. Without privacy, individuals cannot be themselves, and groups need individualism as much as they need conformity. If legitimacy benefits the group, rather than being just a means of control by the few, it is a necessary and pervasive requirement of community development. As has been stated for privacy: "*No-one will take part in the new web-like way of working if they do not feel certain that private information will stay private*." [3]. Businesses should welcome legitimate rights like privacy because they are good for business [18]. But implementing legitimacy concepts in virtual environments offers unprecedented problems, as will now be shown.

Virtual environments are unlike the physical world. Laws in a physical community are expressed in terms of physical actions and concrete objects. They govern what people do, not what they think or feel. Historical law assumes a physical world constrained by time and space. But virtual environments behave significantly differently, both in the scope and nature of activities possible. In the physical world people cannot be in two places at once, but in the electronic world this is as easy as opening two chat room windows. In the physical world to take is to dispossess, but in the virtual world to take is merely to copy. The virtual world is a different world, so it may not be appropriate or even possible to transfer laws from the physical world to an electronic one [5]. They must be, and are being, *re-invented*, by re-applying original legitimate conceptions to virtual environments. In the physical world as one flips TV channels or browses a shopping mall, no-one is recording the commercials you watch or the clothes you try on, but Net browser cookie functionality means the equivalent happens to online surfers. Why this makes some people, as PC World describes it, "mad as hell", is that *they do not feel it is right* [36]. Is setting a cookie on a user's hard drive like a shop slipping their business card in a visitor's pocket, and then surreptitiously checking the pockets of everyone who visits? While for the law, cookies are a new problem, in legitimacy terms the issue is an old one, namely: When is it acceptable to record activity? Virtual environments may require new laws, but basic legitimacy concepts still apply. However while historical law has had hundreds of years to evolve, cyber-law does not have that luxury.

Virtual environments are not like each other. Each VCE designer fashions their virtual world according to their social world view of what is best or right [34]. They can do no other, since the VCE mediates all actions, and must do so in a defined way. But while each designs their virtual society in their own image, the images are not the same. The virtual environment is not one but many, and virtual worlds differ not only from the physical world,

but also from each other. By analogy, in computer simulation games, where players manage virtual worlds, the basic objects, actions and rules of each world may differ. Where virtual environments differ significantly, they in effect require different laws. Given the rate of invention of new, unprecedented virtual situations, it is likely that technology progress will outstrip its social assimilation into law, if it has not done so already. After cookies, what will be the next new software "feature"? As new capabilities appear almost every month, legislative endeavors seem destined to be always behind the play.

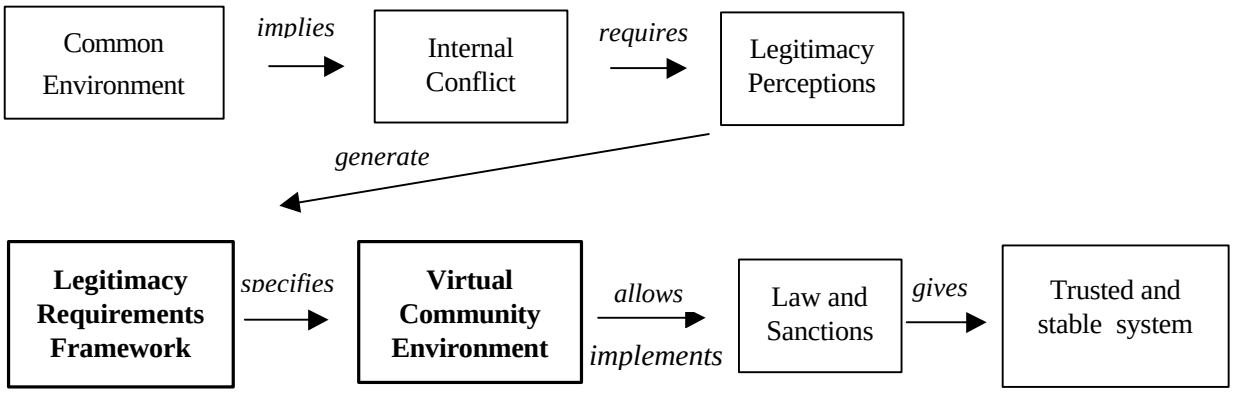

Figure 2. Legitimacy as a basis of virtual community design

Virtual environments can be the law. Since in a virtual community the software defines what objects and actions are possible, it can define and implement legitimacy. Software architecture can regulate people's online lives as much as any tyranny, and while it was originally thought the Net was innately ungovernable, and beyond controls, it is now clear it can easily be "turned" the other way - to a system of perfect regulation and control [17]. As Mitchell so clearly puts it, in cyberspace *code is law* [23, p111], and virtual environments can internally be, and do, whatever their designers wish. By acts of commission and omission, the creators of today's cyber-worlds can implement or nullify any legitimacy concept, e.g. if everyone is anonymous, there is no accountability. If groupware designers are social designers, they are judge, jury, and executioner on issues of legitimacy.

To summarize, while implementing legitimacy is essential for virtual communities:

1. *Virtual environments are unlike the physical world* - they require new laws, re-invented from basic legitimacy concepts.
2. *Virtual environments are not like each other* - each new environment creates new situations that require new laws be re-invented again.
3. *Virtual environments can be the law* – as VCE systems control all system activities, legitimacy considerations may be effectively decided once the system is written.

Perhaps for the first time in human history, we are creating worlds we exist within. While the issues of cooperative community living are old, the possibilities of virtual environments are new. This combination of old and new is not inevitable progress, but a choice: to better implement legitimate rights, acquired through an often painful physical history, or the danger of bypassing them altogether. The power of code is a double edged sword. Facing this challenge, traditional mechanisms of implementing trusted systems seem ill-suited. The law is in danger of becoming often inapplicable, usually out of date, and regularly bypassed in practice, given the rate of software innovation and the power of code to define the online social environment. To develop stable online communities, for trade or any social interaction, requires a new approach.

A solution – legitimate by design

To treat legitimacy as an ethical problem places the onus on the individual. To treat it as a legal problem places the onus on law makers. To make it a social problem places the onus on social action groups. However once the software is written, and the social environment created, traditional ethical, legal and social forces may be ineffective. Legitimacy has thus also become a system design problem. If groupware designers inevitably also design *social systems*, social design requirements must be applied *before* the environment is created, not only after, as has historically been the case (see Figure 2). This resolves the earlier problems. Firstly, legitimacy concepts would be fitted the computer situation if they are designed in. Secondly, if legitimacy is expressed in system design terms it could set a design pattern for many systems, including future ones [32]. It would no longer be necessary to re-invent the law for each new software product. Finally, if the code can be the law, then applying the source of law (legitimacy concepts) at the source of code (design) is the only way to achieve socially acceptable systems. Digital audio technology (DAT) gives an example of this approach. DAT allowed unlimited perfect copying of audio tapes,

whereas previously every tape-to-tape copy was degraded. This was a major threat to copyright. Solutions suggested ranged from using police to increasing fines for copying, but a better solution was to alter the DAT machine code so that once again every copy is slightly degraded [27]. When someone copies a CD too many times (i.e. beyond fair usage), quality degrades significantly. Solutions to technology problems can be built into the technology itself.

Legitimacy requirements framework (LRF). Given a general model of group interaction [38], rights to act can be analyzed as generic IS actions within generic social processes. Legitimacy concepts can be translated into structural and functional system requirements, e.g. authorship rights imply a register of users and a logon process. A LRF can thus express the design requirements for legitimate VCE systems, not just for copy or privacy rights, but all rights (which designers must know). We now present cases to illustrate these concepts, before defining and presenting them in a LRF.

Legitimacy cases

The following examples illustrate how VCE design choices become legitimacy problems. The next section will show how design alternatives could solve these problems.

Case 1. Right to oneself. In Lamda MOO, a text based virtual reality, a character called Mr. Bungle, (actually a group of NYU undergraduates), acquired the power of "voodoo", the ability to take over the voices and actions of other players [9]. Mr. Bungle used this power in public to control and violently "rape" several female characters, making them respond as if they enjoyed it. No physical law was broken - there was no physical contact so there was no legal rape. But clearly a fundamental right of social environments was violated - the right to one's persona. The Lambda MOO community, committed to non-regulation, was outraged, but divided on what to do, until one of the "Wizards" deleted the Mr. Bungle character. Many months and 11 ballots later the system was altered to prevent this type of action recurring.

Case 2. The right to anonymity. Lessig describes a thriving online anonymous class discussion that encountered a vicious personal attack on a classmate by a character called IBEX [17]:

"Almost immediately, conversation in the group died. It just stopped. … Until, that is, the victim responded, with an answer that evinced the wounds of the attack. IBEX's words had cut. The victim was angry and hurt and he attacked back. But his salvo only inspired another round of viciousness … [and] other members of the class could not resist joining in."

This single person changed a thriving online community into a dying one, as people drifted away, disgusted with what had happened, and most simply left the space. Anonymity effectively gave IBEX the right to hurt others, and words can hurt as much as deeds, without accountability. Unable to resolve its internal conflict, the community died, as unlike the Lambda MOO programmers, its members could not redesign their environment to solve the problem.

Case 3. Rights to display. Who happens when one person creates objects within a "space" owned by another? Consider a bulletin board (or chat-room, list server, video-conference etc) created by person P1 for some purpose. Now suppose person P2, who has contributed to the board for some time, adds an item that P1 considers offensive, and P2 refuses to retract it. Does P1 have the right to delete the item? Programming this capability is not difficult. The difficult question is whether it is legitimate. If P1 can destroy the item (and P2's effort in creating it), is not every item potentially deletable, by P1 simply declaring it "offensive"? Surely individuals have rights to the items they create? But if they do, then anyone can add offensive material to any board. Simply deleting the item however may not be enough, as P2 could re-post it. Does P1 also have the right to delete P2 as a person? If so, who now owns any items P2 added that were not offensive? Are these now "orphans", or does P1 now own them? If one person can be "removed", can anyone be removed by the board owner? For most current boards, the controller has all these rights and more, i.e. they are effectively designed as dictatorships, albeit presumed benevolent ones. This is unlikely to be a permanent solution.

Case 4. Rights and sub-rights. These issues are magnified if a "super" bulletin board allows members to create new boards within the main board. If P1 owns the main board, and P2 creates a board within it, who has rights to items in the sub-board? Do *both* P1 (the board owner) and P2 (the sub-board owner) have the right to remove offensive

items from P2's board? What if they disagree? And what if P3 creates a board within P2's board which is within P1's board? This is a serious design issue for multi-level boards.

Case 5. Commenting rights. Where a source item is commented upon, changing the source may change a comment's meaning. What then happens to the comments? For example an item proposing a bid for $1,000,000 might receive the critical comment: "This is too expensive". If the item is now changed to a bid for $1,000, the comment becomes quite inappropriate. Systems which allow such "unfair" actions (e.g. Web-Board) could be considered untrustworthy.

Case 6. Conversation rights. With e-mail, a "private" message addressed to a co-worker can be responded to with a carbon copy to any number of others, and a copy of the original message included. This is the FTF equivalent of every conversant having a tape-recorder and the ability to replay (and broadcast) any prior conversation. A "private" email conversation can so easily become a public broadcast. Yet most people would be upset to see their private e-mails broadcast publicly, on television for example. Is this legitimacy concern merely a convention that new media will overturn? Probably not. More likely problem cases will resurface the issue until private conversations become private. Until then, many may neither trust nor use email for personal messages. President Bush's decision not to use e-mail seems an example.

Some legitimacy concepts

Problems like the above cannot be solved by technology advances. Indeed technology advances, such as mobile computing, are likely to create new legitimacy issues, and compound current ones [12]. The solution proposed is to formally analyse who legitimately owns what from the beginning of system design. We now apply some of the basic concepts of a legitimacy framework to the problems above.

Objects. Since a VCE is an IS, all objects within it are information objects (O). The C3P model suggests generic object types from the three processes [38]. Analyzing task information suggests *item* (representing factual information content), *comment* (semantically dependent items), and *space or container* objects. Relating to other people suggests *mail* (addressed item), *reply* and *conversation* objects. The normative (or group action) process suggests *group, membership, voting* and *vote* objects

Social environment. If a VCE is a social environment (E), it must contain *person objects, or persona, (P)* that *represent* people who also exist in outside the VCE, and can "exist" within it at certain times. A basic legitimacy axiom is that *people have choice and are responsible or accountable for their actions*, e.g. the owner of an item is responsible for its content. Accountability means that all VCE actions must be able to be traced back to people. There is no absolute right to anonymity in communities. A person may be anonymous to others, but must be known to the VCE system or there is no accountability.

Rights. IS functionality is essentially actions upon information objects. System permission for a person to carry out some action upon an information object is a *right.* Specifying what is legitimate means, in system design terms, specifying rights, i.e. *who can/should do what to what, and when*.

Ownership. Ownership in IS terms is having all rights to actions *on or with an object*. To "own" an object yet have no rights to act upon it, or use it, is a contradiction in terms. Over twenty years ago Hiltz and Turoff note that "The first and foremost issue is that of ownership. Who owns the material entered in a group communication space?" [14, p505]. Legitimacy then is about who owns what. While system designers are not concerned with ethical rights or wrongs, a morally neutral VCE may not be an option [4]. A computer system is by its nature fully specified, so who owns what must also be specified. *All changeable VCE objects must be owned by one or more people*.

No rules? The simplest approach is to allocate all rights to everyone - the so called no rules solution. But if everyone has the right to destroy an object, the first to use that right, and destroy it, denies the right to others, as the object no longer exists. To give rights to all is to deny the rights of most. While no rules is an easy implementation, it makes rights an issue of "first in first served", which, like "might is right" in the physical world, is not a good solution socially. If an action changes an object, a VCE must grant unique rights, and only legitimacy gives a valid basis for this.

Ownership of people. Who should own a persona? In the physical world for one person to own another is slavery, and this is now considered illegitimate. Freedom in a virtual context means a persona should belong entirely to the person it represents. One person should not delete, change, use or even view another's persona without their permission. The concept seems simple, yet many systems ignore it, allowing a VCE controller to delete community members. Recognition of this right would preclude a system allowing Mr. Bungle's actions in Case 1.

Spaces. A "social space" (S), or container, is a "mini-environment" which constrains the objects of communication, and thus who communicates with whom [15]. It could be a list, a document, a bulletin board, a drawing area, etc. It is a complex object (one that contains other objects) such that deleting S deletes the O's in it. The system environment (E) is the first S. It follows that *all objects must be contained, and exist within a space*. A space may be *open* or have *restricted* entry, by name or password, as set by the space owner. If one can view an O in a space without entering it, the space is *transparent*, otherwise it is *opaque*. A space owner with the right to refuse entry could have resolved Case 2 by excluding IBEX. While nicknames means people are not accountable in the real world, they are still accountable within the virtual environment, and the sanction of community exclusion remains a powerful one [21]. The right to exclude is not equivalent to the right to delete a persona. Indeed to exclude means *not* to delete, as the system must record who is rejected. If only individuals could own objects, every space would be a dictatorship, but groups can also own objects, and hence spaces. In Case 2, if the group owned the space, it could have voted to eject IBEX and done so.

Delegation and transfer. Ownership rights can be voluntarily transferred. Where a right involves no responsibility for existing information it can be freely transferred, e.g. the right to create. Where a right involves responsibility for existing items, both parties must agree to the transfer, i.e. the original owner relinquishes object ownership, then the new owner takes it up. The full transfer of ownership (all action rights to an object) is non-reversible, as transferring ownership is itself an action upon an object. However the owner may *delegate* an object by transferring all rights to it except the right to transfer ownership. In this case, they can take back object ownership, and the delegatee cannot further transfer ownership.

Object state. A state is the set of actions that can be performed upon an object. Objects can exist in a variety of states. The normal state is "active". But in ownership transfer, after the original owner relinquishes ownership they cannot still change the item. In the "given away" state the only action possible is "take ownership", by either the original or new owner(s). After this, the object returns to the state of "active". States define *when* actions can occur.

Object creation. When an object is created it becomes part of the first complex object that contains it, which changes that complex object. Hence creation is *an action upon the space the object is created in, so the right to create objects in a space belongs initially to the owner of that space.* Others can only create if that right is delegated to them, and delegated rights can always be withdrawn. This provides another solution to cases where an individual is using their right to create to abuse others, as IBEX was in Case 2.

Ownership of created objects. Who owns an object created in a space – its creator or the space owner? Locke stated that an object's creator legitimately owns it. They may give it away or sell it if they choose, but they made it, so they have first rights to it. A space owner cannot both delegate and not delegate creation rights, and so does not directly own objects created by others within their space. Again while this idea seems simple, most current systems ignore it, allowing system controllers to delete, even edit, items in their spaces. Some systems, like WebCT, do not even allow item creators to edit. Yet most do not allow authorship changes, recognizing attribution rights if not copy rights.

Display rights. Displaying an object is an action of the displayed object upon its space. Where one object acts on another, the right to that action resides with both owners jointly. Hence the right to display within a space depends on both item and space owners. An equivalent physical situation is where a notice is placed on a notice board. The board owner may remove it, or the notice owner may withdraw it. But the board owner does not own the notice. They may remove it, but not destroy or change it. Distinguishing display and content rights balances the rights of space owners and item contributors, and resolves the problems of Case 3. If a rejected item is not actually deleted, its owner will still see it (though others wont). If it is deleted, they may think there was an error (on their part or the system's) and resubmit it, unaware it is "rejected". If, knowing it was rejected, they resubmit it, they may risk

exclusion. If they still own the rejected item, they can amend it, and ask again that it be displayed. Carefully following legitimacy concepts gives a better designed social interaction.

Spaces within spaces. Who can create spaces within a space? Suppose P2 can create a space S2 within a space S1 owned by P1, and P1 ≠ P2. P1 owns the content of S1 but has delegated the right to create objects in it. P2 created and owns S2, so can create objects in it. Now suppose P1 takes back the delegated right to create objects in S1. The content of S1 should no longer be changeable by others. However P2 still has the right to create objects in S2, which alters the content of S1 (because S2 is a part of S1). *Hence only a space owner can create a space within their space* (which space they may *then* delegate to another). They cannot transfer ownership of a sub-space, or delegate the right to create sub-spaces, without in effect losing ownership of the space. P1 has no rights to objects within S2 while P2 owns it. But P1 can take back the delegated ownership of S2 at any time, which returns ownership of S2 to P1. P2 is responsible *for* S2, but responsible *to* P1. This resolves the problems of Case 4.

Comments. Suppose the meaning of an object, O2, depends upon the meaning of a *source* object, O1. To process O2 correctly one must first process O1, e.g. the statement "No" may depend on the question "Do you want to come?". Full semantic dependency means if O1 is destroyed, O2 must be destroyed, and if O1 is changed, the meaning of O2 becomes indeterminate (possibly invalid). Items intended to be semantically dependent are *comments or responses.* Non-comment items can also be semantically dependent, but are presumed able also to stand alone. For a comment, this presumption is reversed, that it cannot stand without its source. If the source content is changed, the right to display a dependent comment must be taken back, until the author *reconfirms* it. It should not however be deleted. Such contextual display rights resolve the issues of Case 5.

Conversations. While an idea may have one author, conversations have two or more, suggesting mutual information rights. However current e-mail systems give all rights to the receiver (Case 6). One could design software that recognizes sender rights, e.g. if senders could permanently record "Personal for: xxxxxx" within an e-mail. Interestingly, other conversational conventions are strictly held to, e.g. that one cannot "edit" past messages. In a spoken conversation, what is said cannot be unsaid. This is a property of the airwaves. But with email it would be easy to allow message editing - simply overwrite the previously sent message. But this would contradict the view that the receiver "owns" the sent message. Now imagine a system where the message remains on the sender machine, and only a link is sent to the receiver(s). Message ownership then remains with the message sender, who retains the right to edit or delete "sent" messages at any time, and can also restrict access when the link is activated. The current architecture of e-mail is not a given, it is just one possible alternative. Considering the rights of both senders and receivers suggests alternative designs that could resolve the problems of Case 6. Systems that ensure e-mail goes only to the intended recipient are already available [41].

Group action. To allow groups to act, decide, and own objects is the challenge of the next generation of groupware [38]. Many current systems involve groups, but tend to give them few rights, although group action rights underlie the democracy we live in. If a group does not see the results of their vote on an issue, which goes to some controller, it is a controlled group rather than an autonomous one. Whoever controls the vote result effectively owns it. *Autonomous groups own their own vote information*, so would automatically see the completed vote results. In an anonymous vote no-one, not even a system controller, would know who voted

Object Type	Action upon it	Right
Persona	*Destroy, change*	Of person represented to own their persona (freedom)
Persona	*Display*	Of person represented to control personal information display (privacy)
Object	*Destroy, change*	Of object owner to act upon it (property rights)
Object	*Transfer, delegate*	Of object owner to transfer all or some rights to an object
Space	*Create object in a space*	Of creator to own their creation (intellectual property)
Space	*Entry*	Of space owner to control entry (trespass)
Space	*Create sub-space*	Only a space owner can create a sub-space (c.f. tenants cannot sub-let)
Space	*Display in a space*	Of space owner to display in that space (publishing rights)
Item	*Display an item*	Of item owner not to display their item (copyright)
Comment	*Display a comment*	Of comment owner to assume context (right to be quoted in context)
Membership	*Destroy, create*	Of the group owner to join or eject group members (group right)

Table 1. Some virtual community legitimacy requirements

which way. The group could change the anonymity, but this would release vote authorship to the entire group. While in the physical world, social groups must for practical reasons elect representatives to act for them, virtual groups could act directly, using computer power to calculate vote results for every decision [39]. The group itself could be the actor, not an outside controller using the group. After e-commerce the next revolution may be e-government [33].

A legitimacy requirements framework

The legitimacy concepts discussed are summarized in Table 1. In modern multi-user software, legitimacy requirements must be implemented from the beginning of system design. To give all rights to a single system controller, or to give all rights to everyone, are simple solutions that no longer suffice. A godlike system controller is not only easily overloaded, but has rights others consider unfair. The alternative, and we seem to be developing this way, is to delegate and share ownership rights in complex ways that are commonly accepted. Table 1 is not definitive or complete, but something others can use, build on, modify or even contradict. A full framework would be more detailed than can be covered here.

What is envisioned is not a linear, closed set of absolute rights. Rights can be delegated and taken back, objects may contain other objects, objects may be dependent, rights may interact, groups may have rights, and there may be rights to rights, allowing tailorable systems [34].

A right may be supported without being enforced, by developing socially "translucent" systems, where what one does is (legitimately) visible to others [10]. The action of *viewing* an object has not been discussed. Although viewing doesn't alter the object viewed, it is socially important, as web site counters illustrate. In psychology, the effect of being viewed, or social facilitation, is a powerful one [11, 40]. In an IS system any action can be recorded, and in so doing, it becomes an information object, immediately raising the issue of who has rights to that object. This will be perhaps one of the most complex questions that future social system designers will have to address.

Conclusion

Although social interaction is complex, one thing is clear. Those who create social environments have a responsibility to the community that goes beyond that of a software tool creator. A social environment should not be a Pandora's box, whose contents only become apparent when opened. The social requirements of communities pre-date computer technology, and must be respected. While new technologies cannot in themselves solve old problems like community conflict, they do provide new opportunities to address them. Virtual community environments are such an opportunity, to apply legitimacy concepts, or to ignore them. This is both a research and an educational issue. With the evolution of groups as owners and actors, and the possibility of communities that can decide their own destinies, clarification of social rights will become even more critical. While any rights considered are open to discussion, considered they must be. As Tim Berners-Lee says: "… technologists cannot simply leave the social and

ethical questions to other people, because the technology directly affects these matters." [3, p124]. We can no longer design social software in a social vacuum – it is time virtual community environments were *legitimate by design*.

References

1. Ackerman, M.S., *The intellectual challenge of CSCW: The gap between social requirements and technical feasibility*. Human Computer Interaction, 2000, **15**: p179-203.
2. Adams, J.S., *Inequity in Social Exchange*, in *Advances in Experimental Social Psychology*, L. Berkowitz, (Editor), 1965, Academic Press, New York. p267-299.
3. Berners-Lee, T., *Weaving The Web: The original design and ultimate destiny of the world wide web*. 2000, New York: Harper-Collins.
4. Brey, P., *The ethics of representation and action in virtual reality*. Ethics and Information Technology, 1999, **1**(1): p5-14.
5. Burk, D.L., *Copyrightable functions and patentable speech*. Communications of the ACM, 2001, **44, February**(2): p69-75.
6. Davis, R., *The digital dilemma*. Communications of the ACM, 2001, **February/44**(3): p77-83.
7. de Moor, A., *Empowering Communities: A method for legitimate user-driven specification of network information systems*, in *Dutch Graduate School for Information and Knowledge Systems*. 1999, Tilburg University. p261.
8. Diamond, J., *Guns, Germs and Steel*. 1998: Vintage.
9. Dibbell, J., *A rape in cyberspace*. Village Voice, 1993, **36, 37**(December 23).
10. Erickson, T. and Kellog, W., *Social translucence: An approach to designing systems that support social processes*. ACM Transactions on Computer-Human Interaction, 2000, **7**(1, March): p59-83.
11. Geen, R.G. and Gange, J.J., *Social facilitation: Drive theory and beyond*, in *Small Groups and Social Interaction*, A.P.V.K.M.D. H. H. Blumberg; Hare, (Editor), 1983. p141-153.
12. Ghosh, A.K. and Swaminatha, T.M., *Software security and privacy risks in mobile e-commerce*. Comm. of the ACM, 2001, **February/44**(2): p51-57.
13. Hamman, R.B., *Computer Networks Linking Network Communities*, in *Online Communities*, C. Werry and M. Mowbray, (Editors), 2001, Prentice-Hall: Upper Saddle River, NJ. p71-95.
14. Hiltz, S.R. and Turoff, M., *The Network Nation: Human communication via computer*. Revised edition (from 1978) ed. 1993, Cambridge: MIT Press. 557.
15. Latane, B. and L'Herrou, T., *Spatial clustering in the conformity game: Dynamic social impact in electronic groups*. Journal of Personality and Social Psychology, 1996, **70**(6): p1218-1230.
16. Lau, T., Etzioni, O., and Weld, D., *Privacy interfaces for information management*. Comm of the ACM, 1999, **42**(10): p89-94.
17. Lessig, L., *Code and other laws of cyberspace*. 1999, New York: Basic Books.
18. Lester, T., *The reinvention of privacy*. The Atlantic Monthly, 2001, **March**: p27-37.
19. Lind, E.A. and Tyler, T.R., *The Social Psychology of Procedural Justice*. 1988: Plenum Press, New York.
20. Locke, J., *Second treatise of civil government*. Vol. Chapter 5, section 27. 1690.
21. MacKinnon, *Punishing the Persona*, in *Virtual Culture: Identity and Communication in Cyber Society*, S.G. Jones, (Editor), 1997, Sage: Thousand Oaks, CA. p262.
22. Manes, S., *Private Lives? Not Ours!* PC World, 2000, **June**: p312.
23. Mitchell, W.J., *City of Bits Space, Place and the Infobahn*. 1995, Cambridge, MA: MIT Press.
24. Preece, J., *Online Communities: Designing Usability, Supporting Sociability*. 2000, Chichester, England: John Wiley &Sons.
25. Rawls, J., *Justice as Fairness*. 2001, Cambridge, MA: Harvard University Press. 214.
26. Regan, P., *Legislating privacy, technology, social values and public policy*. 1995, Chapel Hill, NC: University of North Carolina Press.
27. Reidenberg, J.R., *Governing networks and rule making in cyberspace*. Emery Law Journal, 1996, **45**: p911.
28. Rheingold, H., *The Virtual Community: Homesteading on the Electronic Frontier*. 1993, Reading, MA: Addison-Wesley.

29. Rosson, M.B. *I Get By With a Little Help From My Cyber-Friends: Sharing Stories of Good and Bad Times on the Web*, in Proceedings of the 32nd Hawaii International Conference on System Sciences. 1999, Hawaii: IEEE.
30. Schubert, P. *The pivotal role of community building in electronic commerce*, in Proc. of the 33rd Hawaii Intnl Conf.on System Sciences. 2000, Hawaii.
31. Stamper, R., *Social norms in requirements analysis: an outline of MEASUR,*, in *Requirements Engineering: Technical and Social Aspects*, 1994, Academic Press. p107-139.
32. Stefik, M., *Trusted systems.* Scientific American, 1997, **March**: p78.
33. Symonds, M., *The next revolution: After e-commerce, get ready for e-government.* Economist, 2000, **24**(June).
34. Turoff, M., *Computer-mediated communication requirements for group support.* Journal of Organizational Computing, 1991, **1**: p85-113.
35. Tyler, T. *Deference to group authorities: Resource and identity motivations for legitimacy*, in Society of Experimental Social Psychology Annual Conference. 1999, St Louis, Missouri.
36. Tynan, D., *Privacy 2000: In Web we Trust?* PC World, 2000, **June**: p103-116.
37. Weltry, B. and Becerra-Fernandez, I., *Managing trust and commitment in collaborative supply chain relationships.* Communications of the ACM, 2001, **June/44**(6): p67-73.
38. Whitworth, B., Gallupe, B., and McQueen, R.J., *A cognitive three process model of computer-mediated groups: Theoretical foundations for groupware design.* Group Decision and Negotiation, 2000, **9**(5): p431-456.
39. Whitworth, B. and McQueen, R.J. *Voting before discussing: Computer voting as social communication*, in Proc. of the 32nd Hawaii Intnl Conf. on System Sciences. 1999, Hawaii: Hawaii.
40. Zajonc, R.B., *Social facilitation.* Science, 1965, **149**: p269-274.
41. ZixMail, *www.zixit.com*, . 2001.